This Page Is Inserted by IFW Operations and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents will not correct images, please do not report the images to the Image Problem Mailbox.

(54) PIPELINE CONTROL SYSTEM

(11) 58-219646 (A)

(43) 21.12.1983 (19) JP

(21) Appl. No. 57-100706

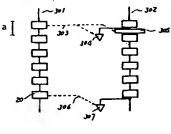
(22) 14.6.1982

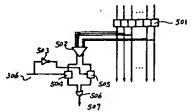
(71) HITACHI SEISAKUSHO K.K. (72) TADAAKI ISOBE

(51) Int. Cl3. G06F9/38

PURPOSE: To detect out of synchronism between plural pipes, by inserting an abnormal data pattern into a stage in an empty state from a control pipe at the entrance of a controlled pipe, and checking the data pattern at the exit of the pipe.

CONSTITUTION: A parity check is made at the entrance of the control pipe 301 and if information in the stage indicates significance, it is stored in a register for the parity check 304 by a signal 303. When it indicates insignificance, a parity error pattern is inserted. The parity check is made even at the exit 20 of the pipe 301; the information is stored in a register 504 when a signal 306 indicates the significance of the information or in a register 505 when not. When there is no out of synchronism between the pipes 301 and 302, a detection signal 507 shows 0. When out of synchronism occurs, the signal shows 1.





a: 1 stage

(54) DIVIDING DEVICE FOR GALOIS FIELD

(11) 58-219647 (A)

(43) 21.12.1983 (19) JP

(21) Appl. No. 57-102803

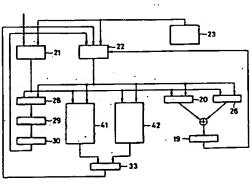
(22) 15.6.1982

(71) TOKYO SHIBAURA DENKI K.K. (72) JIYUN INAGAWA(2)

(51) Int. CP. G06F11/10,G06F7/52,G11B5/09

PURPOSE: To simplify the constitution of a device and to speed up processing, by providing an error location polynominal calculator part with a mutiplying and a dividing device which perform the multiplication and division of a Galois field without providing a logarithm and an antilogarithm buffers.

CONSTITUTION: The order controller 23 of the error location polynominal calculation part of the multiplying device sends an indication of arithmetic order to syndrome and working buffers 21 and 22, and the multiplying device 41 and dividing device 42 perform the algebraic operation of a Galois field GF(2^m). The need for the logarithm buffer and antilogarithm buffer of this polynominal calculator part is eliminated for the multiplication and division of the Galois field GF. The dividing device for the Galois field consists of a linear shift register, gate circuit, plural multiplying circuits, etc., and thus the constitution is simplified to speed up the processing.



19: C register, 20: A register, 26: B register, 28: H register, 29: OR circuit, 30: M register, 33: G register

(54) DIVIDING DEVICE FOR GALOIS FIELD

(11) 58-219648 (A)

(43) 21.12.1983 (19) JP

(21) Appl. No. 57-102804

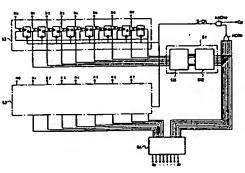
(22) 15.6.1982

(71) TOKYO SHIBAURA DENKI K.K. (72) JIYUN INAGAWA(2)

(51) Int. Cl³. G06F11/10,G06F7/52,G11B5/09

PURPOSE: To realize a small-sized, simplified dividing device, by performing the division of a Galois field without using a logarithm and an antilogarithm buffers which require a large capacity memory.

CONSTITUTION: An error location polynominal calculator part is provided with a multiplying device and a dividing device which perform the multiplication and division of the Galois body GF(2^m). This dividing device is provided with the 1st and the 2nd linear shift registers 52 and 53 wherein one element is set as divident data and the other one is set as divisor data individually. Further, a converter 51 is stored with a table of reciprocal data on elements at specific positions in every of (m) division of 2^m elements in total and a logical circuit decides on whether the reciprocal of the divisor data set in the register 53 is stored in the converter 51 or not. Then, the outputs of the registers 52 and 53 are multiplied by the specific number of times at a multiplier 54 to simplify the dividing device without using a logarithm and an antilogarithm buffers which require a large capacity memory.



PATENT ABSTRACTS OF JAPAN

(11)Publication number:

58-219647

(43) Date of publication of application: 21.12.1983

(51)Int.Cl.

G06F 11/10 G06F 7/52 G11B 5/09

(21)Application number : 57-102803

(71)Applicant: TOSHIBA CORP

(22)Date of filing:

15.06.1982 (72)Inventor

(72)Inventor: INAGAWA JUN

NANUN MASAHIDE

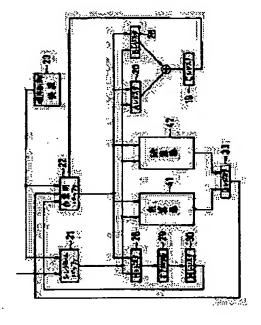
KOJIMA TADASHI

(54) DIVIDING DEVICE FOR GALOIS FIELD

(57)Abstract:

PURPOSE: To simplify the constitution of a device and to speed up processing, by providing an error location polynominal calculator part with a mutiplying and a dividing device which perform the multiplication and division of a Galois field without providing a logarithm and an antilogarithm buffers.

CONSTITUTION: The order controller 23 of the error location polynominal calculation part of the multiplying device sends an indication of arithmetic order to syndrome and working buffers 21 and 22, and the multiplying device 41 and dividing device 42 perform the algebraic operation of a Galois field GF (2m). The need for the logarithm buffer and antilogarithm buffer of this polynominal calculator part is eliminated for the multiplication and division of the Galois field GF. The dividing device for the Galois field consists of a linear shift register, gate circuit, plural multiplying circuits, etc., and thus the constitution is simplified to speed up the processing.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

(9) 日本国特許庁 (JP)

40特許出願公開

⑩公開特許公報(A)

昭58—219647

(1) Int. Cl.³
G 06 F 11/10

G 11 B

識別記号

102

庁内整理番号 7368-5B 砂公開 昭和58年(1983)12月21日

7056—5B D 7629—5D

発明の数 1 審査請求 未請求

(全 16 頁)

60ガロア体における除算装置

7/52

5/09

夏昭57—102803

②出 醇

②特

魔 昭57(1982)6月15日

の発明 者 稲川純

横浜市磯子区新磯子町33番地東 京芝浦電気株式会社音響工場内

70発 明 者 南雲雅秀

横浜市磯子区新磯子町33番地東京芝浦電気株式会社音響工場内

砂発 明 者 小島正

横浜市磯子区新磯子町33番地東 京芝浦電気株式会社音響工場内

砂出 願 人 東京芝浦電気株式会社

川崎市幸区堀川町72番地

仍代 理 人 弁理士 鈴江武彦

外2名

era den de

1. 発明の名称

ガロア体化おける歌舞袋配

2. 特許請求の範囲

ガロア体 GP(2m)にかける 2m個の元のうちの3個 の元α¹,α¹(但しα は 法多項式 P(x)の根)間の飲算 al +al +αl·al·al·αM(但しMは整数) なる 解 1 の長葉 [al·am] および銘2の景集 [aj·am] の函。 の形に変換し、前配第2の乗算がα^j·α^x=α^{2²-1}= $\alpha^0 = 1$ なることを利用して結果的に $\alpha^1 + \alpha^2 = \alpha^1 \cdot \alpha^M$ なる景算に変換して処理するもので、前記元の! が被除数アーメとして直接あるいは遮数何の α^{N1} , α^{N2} ······ 乗算回路(促し)N1 , N2 ····· は 1≤N1 (Ng ·····) を介してそれぞれ毎K セットさ れると共化1シフト毎にそれぞれα^{No} (低しNoは 1 (No.)を乗算する形式になされた第1の譲形 シフトレメスタ群と、前記元 α^{1} が放数アータと して直接 **あるいは 遊数値の a^{ML} , a^{ML} …… 乗** 算回 路を介してそれぞれ毎にせっりされると共に1 シフト毎にそれぞれ a^{Ne} を乗算する形式になる

れた第2の線形シフトレジスタ群と、前記第1 の線形シフトレジスタ群の各レジスタ毎の1出 力を検出する1検出回路群と、この1検出回路 群のいずれかで1出力が検出されるまでの必数 回だけ前記第1かよび第2の線形シフトレジス タ群を共にシフトせしめる第1の手段と、前記 第2の線形シフトレジスタ群の各レジスタの 出力と前記1検出回路群の各検出回路レジスタ 出力を導出する第2の手段とを具備してえることを特徴とするガロア体における除算を

3. 発明の詳細な説明

(発明の技術分野)

との発明は例えば充学式アジタルオーディオ ディスク (DAD) 再生設置等に用いられるエラー 訂正符号の復号用に好適するがロア体における 飲算装置の改良に関する。

(発明の技術的背景)

関知のように、近時開発されている光学式 DAD 再生装置(幹には C D : コンパクトディス

特圍昭58-219647(2)

ク形)においては、そのエラー訂正符号として クロスインまーリープリードソロモン符号 (CIRC)を採用している。

すなわち、これは従来より知られている代表 的なランタムエラー訂正符号のうちで最もエラー 訂正能力が高いものとして広範に定義されてい る BCH 符号の一種であるリードソロモン符号を 用いるものであるが、それにパーストエラーに 対しても高い訂正能力を持たせるべくクロスイ ンタリーアなる信号処理を作わせるようにした ものである。

ところで、リードソロモン符号の復号つまり エラー訂正は BCH 符号のそれと同様になすこと ができる。

今、符号長(n)、情報シンポル(x) 個、検査シンポル (n-k) 個からなるリードソロモン符号について、その復号法を調べてみるものとする。但し、上記各シンポルは例例の2 滋ピットつまり2^m 個の元を有する有限体であるガロア体 GF(2^m)の元である。

s; = R(aⁱ) (但しi=0.1…… 2t-1) …… (5) の如く定義したとすると、上記(3)式より

 $B_1 = C(\alpha^1) + E(\alpha^1)$

となる.

この場合、C(x)はP(x)で常に割り切れるので $C(\alpha^1)=0$

てわるから

 $s_i = E(\alpha^i)$

となる。そとで、上記(4)式より

$$\mathbf{g}^{\dagger} = \mathbf{E}(\alpha_{i}) = \sum_{i} \mathbf{A}^{\dagger}(\alpha_{i})_{\dagger} = \sum_{i} \mathbf{A}^{\dagger} \mathbf{X}^{\dagger}_{i} \qquad (e)$$

と表わけことができる。但し $\alpha^{j}=X_{j}$ とかいたもので、 X_{j} は α^{j} 化かけるエラーロケーションを表わしている。

ととで、エラーロケーション多項式 (g) は、 エラー数をりとして

$$\sigma_{(x)} = \prod_{i} (x - X_{i})$$

$$= x^{0} + \sigma_{1} x^{0-1} + \dots + \sigma_{0} \qquad \dots$$
 (7)

と定義される。

また、切式のちゃっぱシンドローム8;との間で

そして、この場合(4) 東エラー訂正リードソロモン符号の生成多項式 (g)は、(内をガロア体 GF(2P)の原始元として次の(1) 式または(2) 式のように表わされる。

$$f(x)^{\infty} (x+\alpha)(x+\alpha^2)$$
 $(x+\alpha^2)$ (1)

$$F(x)^{-1}(x+\alpha^0)(x+\alpha)$$
 $(x+\alpha^{2t-1})$ (2)

また、送信符号語を C(x)、受信符号語を R(x)で 表わし、且つエラー多項式を R(x)とすると、これ らの間には次のような関係が成立する。

$$R_{(x)} = C_{(x)} + E_{(x)}$$
(3)

この場合、多項式の係数はガロア体 GP(2^m) に含まれており、エラー多項式 E(x) はエラーロケーションおよび値(大きさ)に対応する項だけを含んでいる。

使って、位置 x^j にかけるエラー値を Y_j とする L

ととて、シンドロームのま

次のように関係付けられる。

8_{1+e}+ σ₁g_{1+e-1}+······ σ_{e-1}g₁₊₁+σ_eg₁ ········ (8) つまり、以上のようカリードソロモン符号の 復号手順は

- (1) (5)式によりシンドローム8,を計算する。
- (団). (8) 式によりエラーロケーション多項式の係数 o₁ ~ o₂ を計算する。
- (7)式によりエラーロケーション多項式の根X: を求める。
- (M) (6) 式によりエラー値 Yj を求め、(4) 式により エラー多項式を求める。
- (V) (3)式によりエラー打正を行なり。
- なる(I) ~.(V) の手版に帰着せしめられる。

次に、以上のような復号手順によるエラー町 正の具体例として、1プロックデータに4個の 検査シンポルを用いた場合について説明する。

すなわち、との場合の生成多項式 F(x) は F(x) F(x)

となり、2<u>款ェラーまでの訂正が可能となるも</u> のであるが、ここではそれを (A) 、 (B) なる二 つの方式によった場合について各別に述べるも のとする。

〔 方式 A 〕

- (1) シンドローム 80~85を計算する。
- (凹) (8)式を e□1, e□2について書き直すと、e□1 の場合には

となる。また 6-2の場合には

$$\begin{cases} 8_2 + \sigma_1 8_1 + \sigma_2 8_0 = 0 \\ 8_3 + \sigma_1 8_2 + \sigma_2 8_1 = 0 \end{cases}$$

となる.

ことで、実際の復号器が 8m 1の場合から動作を始めるものとすると、先ず建立方程式(8)を満足する無。を求めなければならない。そして、この解が存在しなければ、復号器は次に 8m 2 で 2 を求めなければならない。 なか、ここでも解が得られない場合は 6 ≥ 3 とみなすことになる。

先ず、6=1の場合は
8₀=Y₁ : Y₁=8₀
となる。また、6=2の場合は
8₀=Y₁+Y₂

$$\mathbf{S}_1 = \mathbf{Y}_1 \mathbf{X}_1 + \mathbf{Y}_2 \mathbf{X}_2$$

t þ

$$\therefore Y_{1} = \frac{X_{2}S_{0} + S_{1}}{X_{1} + X_{2}}$$

Y2 = 80 + Y1

(Y) 上述のようにして求めたエラー値で。Y2により訂正を行なう。

ところで、ポインターイレージャー法等によってエラーロケーションの値を正確に知ることができる場合には、上述した2重エラー訂正用のリードソロモン符号によって4重エラーまでの訂正が可能となるものであり、それが保述する(方式 B)である。

〔方式 B 〕

- (I) シンドローム Ba~Baを計算する。
- (11) 印 エラーロケーションを別の検出方法で

特周昭58-219647(3)

(9)式の解の,は

$$\sigma_1 = \frac{8_1}{8_0} = \frac{8_2}{8_1} = \frac{8_8}{8_2}$$

として求め、匈式の解の、、の2は

$$\sigma_1 = \frac{s_0 s_3 + s_1 s_2}{s_1^2 + s_0 s_2} , \quad \sigma_2 = \frac{s_1 s_3 + s_2^2}{s_1^2 + s_0 s_2}$$

として求める。

毎 以上のようにしてエラーロケーション多項式の係数 □ が得らたならは、次に(7) 式により
エラーロケーション多項式の機を求める。

先ず、 8=1 の場合は

$$\sigma_{(x)} = x + \sigma_1 = 0 , \quad \therefore X_1 = \sigma_1$$

となる。また、6=2の場合は

(f) エラーロケーション多項式の根が求まったな ち、次に(6) 式によりエラー値 Y₆ を求める。

知る。

(M) (6)式によりエラー値を求める。 ・先すe=1.e=2 の場合は上述した〔方式A〕 のMと同様である。

そして、e=3の場合

$$s_0 = Y_1 + Y_2 + Y_3$$

$$s_1 = Y_1 X_1 + Y_2 X_5 + Y_5 X_5$$

$$s_2 = Y_1 X_1^2 + Y_2 X_2^2 + Y_5 X_5^2$$

+ # W T

$$Y_1 = \frac{(8_2 + x_5 8_1) + x_2(8_1 + x_5 8_0)}{(x_1 + x_2)(x_1 + x_5)}$$

$$Y_2 = \frac{(8_1 + X_3 8_0) + Y_1 (X_1 + X_3)}{(X_2 + X_3)}$$

 $Y_5 = S_0 + Y_1 + Y_2$

となる。

また、 e=4 の場合は

$$8_0 = Y_1 + Y_2 + Y_5 + Y_4$$

$$S_1 = Y_1 X_1 + Y_2 X_2 + Y_3 X_5 + Y_4 X_4$$

$$S_2 = Y_1 X_1^2 + Y_2 X_2^2 + Y_5 X_5^2 + Y_4 X_4^2$$

$$8_5 = Y_1 X_1^5 + Y_2 X_2^5 + Y_5 X_5^5 + Y_4 X_4^5$$

を解いて

$$Y_1 = \frac{[(S_0X_4 + S_1)X_5 + (S_1X_4 + S_2)]X_2 + (S_1X_4 + S_2)X_5 + (S_2X_4 + S_2)}{(X_1 + X_2)(X_1 + X_3)(X_1 + X_4)}$$

$$Y_2 = \frac{(8_0X_4 + 8_1)X_5 + (8_1X_4 + 8_2) + Y_1(X_1 + X_2)(X_1 + X_4)}{(X_2 + X_3)(X_2 + X_4)}$$

$$Y_{4} = \frac{(S_{0}X_{4}+S_{1})+Y_{1}(X_{1}+X_{4})+Y_{2}(X_{2}+X_{4})}{(X_{3}+X_{4})}$$

$$Y_4 = S_0 + Y_1 + Y_2 + Y_3$$

となる。

(M) 上述のようにして求めた Y1~Y4 により 訂正を行なう。

第1図は以上のような原理に善くりードソロ

器11かエラー弦を計算し、これらのエラーロケーションかよびエラー値により上記データペッファ11から出力されるデータを訂正するものである。

ところで、このような復号システムの各計算器 1 ま、1 5、1 6、1 7 は 0 か否かの検出ならびに必要な加算、乗算やよび欲算の代数演算をなすものであるが、これらについての具体例として従来第 2 図に示すように構成されたエラーロケーション多項式計算器 (特公昭 5 6 - 2 0 5 7 5 号) が知られている。

すなわち、終 2 図において 3 1 はシンドローム A パッファであって、シンドローム B i を記憶するための RAM でなり、数シンドロームパッファ 3 1 にはガロア体 GP(2^m) の元である各シンドロームがそれぞれ R ビットの 2 進形式で記憶される。

また、2 3 は作業用ペッファであって、エラーロケーション多項式の係数を計算する原化、 代数演算の中間結果および最終結果を記憶する 特問昭58-219647 (4)

モン符号の実際の復号システムを示す報路構成 図である。すなわち、入力値 (IN)を介して導か れる被訂正用のデータ(エラー訂正用としてリ ードソロモン符号が用いられていることは勿論 である)は二分されて、一方が使述する復母動 作の間データペッファエ』に配像されると共化、 他方が復号動作をなすためのシンドローム計算 器13以下に導かれる。

そして、シンドローム計算器18で計算されたシンドロームはシンドロームペッファ18化配像される。

として、シンドロームパッファ13の出力部 に接続されたオアゲート14はエラーの有級を 指示するもので、エラーがあると前述したよう な手順によってエラー訂正動作を開始すること にかる。

つまり、エラー。ロケーション多項式計算器18 がエラーロケーション多項式 σ(x) の係数を計算 し、エラーロケーション計算器 1 8 がエラーロ ケーション多項式の根を計算し、エラー値計算

ための RAM でなり、後の改算で使用される部分 結果も駄作業用パッファミミに記憶される。

そして、33は代数演算の順序を指示する順序制御装置であって、上記シンドロームパッファ31かよび作業用パッファ33に対してアドレスを供給して遊切な記憶位置をアクセスすると共に、実行された代数演算結果を調べて次の適切な演算へ分数せしめるのに供せられる。

さらに、34・35 社それぞれガロア体GF(型)の元の対数および真数を各別にテープルの形式で記憶している ROM でなる対数パッファおよび 実数パッファである。

とこで、前者の対数パッファミイのアドレス は元α¹ の 2 進長示であり、そのエントリーはα を底とするαの対数すなわち 1 であるが、 徒者 の実数パッファミミのアドレス 1 にかけるエン トリーはα¹ の 2 進表示である。

例えばガロア体 GP(2⁸) の法多項式 F_(x) を F_(x) = x⁶ + x⁴ + x⁵ + x⁴ + 1

とすると、その O 以外の元は P(x)= O の根 a のべ

特质昭58-219647(6)

も乗または a0~a7 までの無形 結合

$$\sum_{i=0}^{7} a_i \alpha^i \quad (\text{(il)} a_i = 0 \pm \hbar \text{(ii)})$$

で表わすととができる。

また、この場合 ap~ay までの8 個の係数を取り出して2 進ペクトルとして扱わすこともできる。

例允は

 $\alpha^{1}=0 \cdot \alpha^{0}+1 \cdot \alpha^{1}+0 \cdot \alpha^{2}+0 \cdot \alpha^{5}+0 \cdot \alpha^{4}+0 \cdot \alpha^{5}+0 \cdot \alpha^{6}+0 \cdot \alpha^{7}$

~(01000000)

 $\alpha^7 = 0 \cdot \alpha^0 + \dots + 0 \cdot \alpha^4 + 1 \cdot \alpha^7$

-(00000001)

a=1+a4+a5+a4

= (10001110)

a 9 = a + a 8 = a + a 6 + a 6 + a 7

= (01000111)

の如くであり、とれら以外の元も同様にしてペ クトル表示することができる。

そして、この場合対数テージルのアドレス (1~255)は元a¹ の8ピットの2 進ペクトル表示

•

がりのときのみりになる。

(3) 乗算

元 al かよび al を乗算する場合には、 先ずとれ 62つの元が0であるか否かが何べられる。若 し、いずれか一方の元がりであれば、実験に乗 算するまでもなく、乗算結果は 0 である。しか るに、両方とも0でない場合には、これらの元 は上記対数パッファミィ用のアドレスレジスタ 3.1 に頂衣にロードされる。そして、対数ペッ ファミィからの出力!および!はDレジスタ88 およびBレジスタ88を介して1の抽数加算器 ♪ 4 により、 28-1 を法として 1 の精散加算が行 なわれる。とれによって得られる結果(1+1)= t mod (2⁸-1) は エレ リスタ & 8 を介して上記真数 パッファミを用のアドレスレジスタミをにロー とされる。この場合、実数パッファ 3.5 のアド レス入力が t であれば、その出力 cf が乗算結果 としてGレジスメ87を介して上記作業用ペッ ファミミに転送される。

であり、対応するエントリは指数1の2 進長示である。

また、真数テープルは指数しをアドレスに用い、エントリは qi の2進ペクトル表示である。

次に、第2回のエラーロケーション多項式計 算器による実際の代数演算を各別に説明する。

(1) 加算

元 al および al を加算する場合には、とれら2つの元がAレジスタ20およびBレジスタ26を介してエクスタルシプオアゲート39により各ピット毎に拚他的な職理和をとる。これによって得られる上記2つの元の和の結果はCレジスタ19を介して上記作業用パッファ22に転送される。

(2) 0 であるか否かの検出

元 a が 0 であるか否かを調べる場合には、元 a が H レ ジスタ 3 8 を介してオアゲート 3 9 に より 論 理和がとられる。 この結果は M レ ジスタ 3 0 を介して上記作業用ペッファ 3 3 に 伝送される。この場合、 M レ ジスタ 3 0 の内容は元 a 1

(4) 除 1

元 a l による a l の飲算 (a l / a l) は基本的には上記 (3)の乗算の場合と同様であるが、上記 E レンスタョョの内容を上記 D レンスタョョの内容を上記 D レンスタョョにある元 a l の対数が構数化器 B l により構数化されて P レンスタョョを介して表にしてある。そして、以下(3)の乗算の場合と関様に処理されるものであるが、この場合真数パッファ25の出力が求める飲算の結果つまり商となっているものである。

(背景技術の問題点)

しかしながら、以上のような従来のエラー訂正装置は、そのエラーロケーシ。ン多項式計算器における代数演算のうち乗算および除算用として対数パッファおよび真数パッファを必要とするものであるが、このために用いられる ROM 等のメモリ容量が膨大なものになるので、 LBI 化が阻害されて大容量のメモリを外付けしまけ

特徵昭58-219647(6)

ればならないという不具合を生じていた。

これは、前述した例の如く 1 シンボル 8 ピットとした場合で 2 5 5 × 8 ピットロ 2 0 4 0 ピットの ROM が 2 つ必要になり、合計 4 0 8 0 ピットにもなることからして容易に扱い知れるところである。

つまり、従来より知られているガロア体にかける乗算機僅かよび除算機置はそれらの元の対数かよび実数を各別にテーブルの形式で記録している大容量メモリでなる対数ペッファや実数ペッファを必要とするので、それだけ構成が複雑化して高価格につくという問題を有していた。 (発明の目的)

そとで、との発明は以上のような点に鑑みてなされたもので、特に大容量のメモリを必要とする対数パッファや実数ペッファを用いることなくガロア体にかける飲算をなし得るようにし、以って構成の信息化ならびに低価格化かよび高速処理化に寄与し得るようにした極めて良好なるガロア体にかける飲算装置を提供することを

目的としてりる。 (発明の観要:)

すなわち、この発明によるガロア体における 映算装置はガロア体 GP(2m)にかける 2m 個の元 のうちの2個の元 α¹ · α¹(但しαは法多項式 F(x) の担)間の除載 al +al を al・a m + al・a m (但し 近は整数) なる第1の乗算 (α1·α×) かよび第2 の乗隻 (aj·a M) の商の形に変換し、前記第2の 景集が $\alpha^1 \cdot \alpha^2 = \alpha^{2^{2^{n}}-1} = \alpha^0 = 1$ なるととを利用して 始果的に $\alpha^{I} \div \alpha^{J} = \alpha^{I} \cdot \alpha^{M}$ なる乗算に変換して処 遠するもので、前記元は が被除数データとして 直接 あるいは 遺数 個 の α^N1 , α^{N2} ······ 乗算回路(但 し N1 , N2 ····· は 1≦N1 (N2 ·····) を介してそれぞ れ缶にセットされると共に1シフト毎にそれぞ れ a No (但しNo は1くNo) を景算する形式になる れた第1の銀形シフトレジスタ群と、前記元01. が飲飲テータとして直接あるいは道数個のです。 α 異類回路を介してそれぞれ毎にセット されると共に1シフト伝にそれぞれ a^{R4} を乗算 する形式になされた第2の線形シフトレジスタ

群と、前配解1の線形シフトレジスタ群の各レジスタ毎の1出力を検出する1検出回路群の公式を検出する1検出回路群のいずれかで1出び第2の1枚出回路群の大け前記第1をよしいの多数回だけが配常1をより、前記第2の部1をより、前記第2の数配1検出回路群の出力とのでは、かられたレジスタ出力を導出している。

(発明の実施例)

先す、との発明が適用される光学式(CD形) アジタルオーティオティスク (DAD) 再生終度の 板裂について説明する。

すなわち、第3回に示すようにディスクモータ』』」によって回転駆動されるターンテープル』』2上に殺着されたディスク』』3仕先学文ピックアップ』14によって再生される。この場合、光学式ピックアップ』14仕半導体レーデュ14。からの出射光をピームスプリッチー

114b、対物レンボ114cを介してディスタ113の信号面に照射し、飲ディスク113に所定の(EFM)変調かよびインタリーアを指った形態で記録されている再生すべきのでは対応したがでは、114c、ピームスアリッター114cを介しても分割フォトアテクタ114cで洗ります。 は4分割フォトアテクタ114cで洗りますれているもので、自からはピックアップを行っているもので、自からはピックアップを行っているもので、2115によりには変数的される。

そして、4分割フォトデテクタエコ 4 d からの4つの再生信号はマトリクス回路エエ 6 に供給されて所定のマトリクス演算処理が施されるととにより、フォーカスエラー信号(P)、トラッキングエラー信号をよび高局政信号(RF)。に分離される。

とのうち、フォーカスエラー信号切はフォー

特別昭58-219647 (プ).

カスサーチ回路!! 0 からのフォーカスサーチ 信号と共化、前記光学式ピックアップ!! 4 のフォーカスサーオ系 (P8) を駆動するのに供せ られる。

また、トラッキングエラー信号的はほ述するシステムコントローラ』」「を介して与えられるサーテ制仰信号と共に、前記光学式ピックアップ」」(のトラッキングサーポ系(TB)を駆動するのに且つ前記ピックアップ送りモータ」」を(リコアトラッキング)制御するのに供せられる。

そして、残る高周波信号(RP)が主再生信号 成分として再生信号処理系<u>118</u>に供給される。 すなわち、との再生信号処理系<u>118</u>は先ず再 生信号をスライスレベル(アイパターン)検出 数 3 1 9 によって制御される波形整形回路 120 に導いて不要なアナログ成分と必要とするデー メ成分を分離し、データ成分の今を PLL 型でな る 同期クロック再生回路 1 2 1 2 4 3 6 に供給 号処理系 1 2 2 0 エック検出器 1 2 3 6 に供給 ことで、何期クロック再生回路 1 2 1 からの 同期クロックはアーチ 復興用として第 1 の信号 処理系 1 2 2 における同期信号分類用クロック

一方、上記エッジ検出器 1 3 3 6 を通った再生信号は同期信号検出器 1 3 2 6 化導かれて上記同期信号分離用クロックにより同期信号が分離されると共に、復興回路 1 2 2 6 に導かれて(EFM) 復講される。

このうち、同期信号は同期信号保護回路1220 を介して誤動作が生じないように保護された状態で、上記同期信号分離用クロックと共に入力 アータ処理用タイミング信号生成回路1221 に導かれる。

また、復認信号はデータパチス入出力制御回路133gを介して接送する第2の信号処理系133の入出力制御回路133mに供給されると共に、そのうちのサプコードであるコントロ

ール信号をよび表示信号成分がコントロール表示処理回路 1 3 3 h をよびサプコード処理回路 1 3 3 i に導かれる。

そして、サプコード処理回路1331で必要なエラー検出かよび訂正が施されたサプコードアーチはシステムコントローラ用インターフェイス回路133gを介してシステムコントローラ117に供給される。

ここで、システムコントローラミミナはマイクロコンピュータ、インタフェイス回路およびドライベ用集教回路等を有してなり、コントロールスイッチミミイからの指令信号により DAD 再生執便を所譲の状態に制御すると共に、上述のサプコード(例えば再生曲のインデックス情報)を投示器ミミミに表示せしめるのに供せられている。

なお、上記入力データ処理用タイミング信号 生成回路 1 2 2 2 2 からのタイミング信号はデー タセレクト回路 1 2 2 3 2 を介して上記データペ 六入出力制御回路 1 2 2 3 を制御するのに供せ られると共に、周波数検出器122kをよび位相検出器122kを分びにPWM 変調器122mを介して上記ディスクモータ111を譲速度一定(CLV)方式で駆動するための自動周波数制物(APC)を供せられている

との場合、位相検出器122Aにはクリスタル発担器122nからの発担信号に基いて動作するシステムクロック生成回路122pからのシステムクロックが供給されている。

そして、終2の信号処理回路122の入出力 制御回路122を通った復興アータはエラー 検出および訂正または補正用のシンドローム検 出器1226、エラーポインタ制御回路1226、 訂正回路1234を介して必要なエラー訂正、デインタリープ、 エラー補正等の処理を受けてデジタル・アナロ タ (D/A) 変換器126に導出される。

との場合、外部メモリ制御回路1231以上 記テータセレクト回路1221と共働して訂正

特開昭58-219647(8)

に必要なアータが書き込まれている外部メモリ 127を制御することにより、上記入出力制御 回路122・を介して訂正に必要なアータを取 り込む如くなされている。

さた、タイミングコントロール回路133g は前記システムクロック生成回路133pからのシステムクロックに基いてエラー訂正および 補正ならびにD/A 変換に必要なタイミングコントロール信号を供給する如くなされている。

また、ミューティング(検出)創御回路133b は上記エラーポインを創御回路123cからの 出力またはシステムコントローラ117を介し て与えられるコントロール信号に基いてエラー 補正時かよびDAD 再生装置の動作開始、終了時 等に必要となる所定のミューティング創御をな すのに供せられている。

そして、上記 D/A 変換器 1 2 6 でアナログ信号に戻されたオーディオ信号はローバスフィルタ 1 3 8、増展器 1 2 9 を介してスピーカ130 を実施するのに供せられる。

次に、以上のような DAD 再生装配のエラー訂正部に適用されたとの発明に係るガロア体における缺算装置の一実施例につき図面を参照して詳細に説明する。

すなわち、第4回は第3回における第2の信 号処理回路188の訂正回路1884尺主とし て含まれる前述したようなエラーロケーション 多項式計算器耶を示しているもので、対数パ。 ファヤ真数パッファを用いるととなくガロ丁体 にかける乗算および除算がなし得るようにした 乗算袋籠41かよび放算袋置48を備えている 以外は前述した第2回のそれと同様である。つ まり、エラー訂正符号として採用された BCH 符 号の一種であるリードソロモン符号の復号(エ ラー訂正)のために各種の代数演算をなすのが エフーロケーション多項式計算器に与えられた 役目であるが、とのうち加算やよび0であるか 否かの検出については第2回のそれと同様にな されるので同一符号を付してその説明を省略す るものとし、前2図のそれとは異なる乗算かよ

び除算について以下に述べるものである。

先ず、ガロア体における乗算についてみてみるに、例えばガロア体 $GP(2^6)$ の元 α^1 と α^1 と α^2 と α 5 件 α^4 と α^5 ,但し α 社 法 多 項式 $P(x) = x^6 + x^6 + x^5 + x^4 + 1$ の根である)は

 $\alpha^{\dagger} = C(\alpha) = e_0 + e_1 \alpha + \dots + e_7 \alpha^7$

a = D(a)= d0+d1a+ d7a7

と終わした場合(但し、 e₀~c₇ , d₀~d₇は 0ま たは 1 とする)

 $\alpha^{j} \cdot \alpha^{j} = C(\alpha) \cdot D(\alpha)$

 $= a_{1} \alpha^{7} C(\alpha) + a_{4} \alpha^{4} C(\alpha)$ $a_{0} C(\alpha)$

 $= a^{4} (\alpha a_{7} C(\alpha) + a_{6} C(\alpha)) + a_{5} a^{5} C(\alpha) + \cdots + a_{0} C(\alpha)$

 $= \alpha^5 (\alpha (\alpha a_7 C(\alpha) + a_4 C(\alpha)) + a_5 C(\alpha)) + a_4 \alpha^4 C(\alpha) + \dots$

----- + 60C(A)

となる。

つまり、とのようなガロア体 GP(2⁶)の元α¹

との 1 との 乗算は 線形 シフトレ ジスタを 用いて 第 5 図に示したように 構成される 乗算袋 置で 実現 し得ることを 物節っている。

すなわち、第 8 図において AND。~AND, は各一 増に上記景数 D(4)の係数である do~d, が上位ヒッ トから頂に シリアルに供給されると共に、各他 増に上記被景数 C(4)の係数である co~c, が上位ヒッ トから頂に ペラレルに供給されるアンドゲー トである。また、 PF®~PF, は、上配各 アンドゲート AND® ~ AND, からの出力が入力一端に対 応して供給されるエタスタルシブオアゲート (EX-OR®)~(EX-OR) を介して提供的に接続されると共に帰還接続されることにより練形シフトンジスタ BB® を構成するフリップフロップ回 略である。

との場合、4 取目と5 取目、5 取目と6 取目 および 5 取目と7 取目のフリップフロップ回路 PFa-FF4, FF4-FFa, FF4-FF7 との取削は各 一端が得遺路に接続されたエクスクルシアオア ケート EX-OR4, EX-OR4, EX-OR4 かさらに介揮

特問昭58-219647 (9)

された状態で始合されている。また、各フリップフロップ回路 PF。~PP;のクロック入力場 C R には図示しないクロック発生器からのクロックがパラレルに供給される如くなされている。

つまり、CMの係数 e₀ ~ e₇ がピットシリアル に入力されることにより、先 す x₀ が計算され、 その後 x₁ , x₂ …… と 使い て 8 ピット入力終了時 に 線形シフトレジスタ B R e に は x₇ すなわち CM・DM が実現されるもので、各フリップフロ ップ回路 P P e ~ P F f の出力(x₀ , x₁ …… x₇) が 果 算 結果を与えることに なる。

ととで、 Xo ~ X7 は次の通りである。

 $X_0 = d_1 C(\alpha)$

 $X_1 = \alpha X_0 + d_4 C(\alpha)$

 $X_2 = \alpha X_1 + \delta_5 C(\alpha)$

 $X_4 = \alpha X_2 + d_4 C(\alpha)$

 $X_4 = \alpha X_5 + d_5 C(\alpha)$

X5 = aX4+42C(0)

 $X_A = \alpha X_5 + d_1 C(\alpha)$

 $x_7 = \alpha x_4 + d_0 C(\alpha) = (x_8, x_1, \dots, x_7)$

と同位である(但し、M は整数)。 この場合、 $\alpha^{j} \cdot \alpha^{N} = \alpha^{255} = \alpha^{0} = 1$ ならば $\alpha^{i} \div \alpha^{j} = \alpha^{i} \cdot \alpha^{N}$ となる。

 $a^1 \div a^1 = (a^1 \cdot a^m) \div (a^1 \cdot a^m)$

そして、以上のようなガロア体 GF(2⁸)にかけ

る景算装置はガロア体 GP(28)の元の対数かよび

実数をテープルの形式で記憶する ROM 等の大容

量メモリでなる対数パッファヤ実数パッファを

用いるととなく、単に線形シフトレジスメを用

いるだけでなし得るので、その構成を簡易で安

価なものとするととができるという効用を有し

次に、ガロア体における験算についてみてみ るに、例えばガロア体 GP(2⁸)の元α¹ とα¹ との

除算α1+α1 (但しαは法多項式P(x)= x8+x4+x5

+24+1 の根とする)は

つまり、ガロア体 $GP(2^8)$ の元 α^i と α^j との飲算 $(\alpha^i+\alpha^j)$ をなす場合、被除数 α^i 、除数 α^j にそれぞれなを何因か乗じて行く過程で、M回なを乗

じたときに a¹・a^M=1に なったとすれば、そのと きにかける被除数 a¹ と a^m との様である a¹・a^M が 味算結果であることに外ならないことを利用し て、乗算処理で所親の除算をなせることになる。

ととで、乗算処理については前述したような 額形シフトレジスタによる乗算装置を用いてな すことは言う泣もない。

ところで、この場合 aJ・a^M = a²⁵⁵ = a⁰ = 1を得るために必要となる a を乗じる回数は、缺数 aJ=a¹ のときに最高で 2 5 4 回(つまり M = 2 5 4)となるが、単純にその通りになせるようにしたのでは乗算処理に要する時間が徒らに長時間化してしまうので好ましくない。

そこで、この発明では被除数 なり、除数 なりに対し予め適数的回だけなを乗じてかくことにより、実際に必要となる なを乗じる回数を低減して短時間で乗算処理(狂いては除算処理)がなせるようにしょうとするものである。

第6回は以上のようにガロア体における除算を乗算処理で実現する除算装置の構成を示すも

ので、この場合上述の図として $N_1=1$, $N_2=2$ 、 $N_3=3$ つまり α^1 , α^2 , α^5 を子め乗じると共化、 $N_0=4$ つまり 1 回係化 α^4 を乗じるようにしたものである。

すなわち、絵数α3アータは直接あるいはα5 乗算回路δ1、α2乗算回路δ2、α5乗算回路 δ3を介してα4乗算回路を構成する線形シフト 、レジスタム1 、A1 、A1 にセットされる。

Cとで、線形シフトレジスタAI 、Aa 、Aa 、Aa 、Aa は第7図に示すようにフリップフロップ回路 F Pi a ~ F Pi a をエクスクルシプオアゲート BX-ORio~ EX-ORai を介して適宜級銃的に且の帰還的に級銃して構成されるもので、アンドゲート ANDio を介して与えられるクロックパルスCp によりシフトされ、1 シフト毎に α^4 が 乗算される如くした α^4 乗算機能を有している。

そして、シフトレジスタ A 1 , A 8 , A 8 , A 8 , A 8 , A 8 , B の各出力が供給される 1 検出回路 5 4 , 8 8 , 8 8 , 8 7 は 第 7 図 に示したよう にイン

特問昭 58-219647 (10)

パータ I 10 と 8 入力ノアゲート NOR 10 によって 構放されているもので、レジスタの内容が (10000000)=1になったときに 1 検出出力 を生じるようになされている。 この 1 検出回路 5 4 、6 8 、6 6 、6 7 の各出力が供給される 4 入力ノアゲート NOR 11 は当故 1 検出出力のい ずれかが生じたときに、その出力が"0°となる ととによって前記アンドゲート AND 10 を介して クロックパルス Cpの通過をそれ迄の許容状類か ら類止状態とする如く制御している。

また、被除数 α^1 アータも上配 数 α^2 アータと 同様に 直接 もるいは α^1 乗 算 回路 δ も、 α^2 乗 算 回路 δ も、 α^2 乗 算 回路 δ ものを 介して 第7 図 に 示したよう な な 4 乗 算 回路 を 構成 する 線形 ν フトレ ν スタ B₁ , B₂ , B₃ , B₄ に セット され た を、 上配 ρ ロック パルズ C_p により α^4 が 連数 回 乗 算 でれる ことに なる。

とこで、シフトレジス点 B_1 , B_2 , B_3 , B_4 の各出力は上記 1 検出回路 5 4 , 5 5 , 56 , 56 , 57 から各出力と対応的化アン F 回路 61 , 63 ,

81,81KID、TYPがとられることにな

そして、アンド回路 6 1 . 6 2 . 6 3 . 6 4 の各出力をオフ回路 6 6 に通すことで、 α^{1} ÷ α^{3} の飲算結果を得ることができる。

係8回は以上におけるアンド回路 61~64 の具体例を示するので、各入力一塊が線形シフトレジスタ Bi ~ B 4 からの各出力が対応的に供給されると共に、各入力他端に1 快出回路 54~57 の各出力が対応的に共通に供給される8 旬の2 入力アンドケート AND 20 ~ AND 21 で構成された場合である。

第9回は以上におけるオア回路 65の具体質を示すもので、上記アンド回路 81~64の各出力が対応的に供給される8個の4入力オアゲート OB29~OB27 で構成された場合である。

親10回は以上におけるα¹乗算回路 δ δ Φ 具体例を示すもので、この場合α¹が

 $\alpha^1=B$ $\Theta=b_7\alpha^7+b_4\alpha^6+\cdots\cdots$ $+b_1\alpha+b_0$ で扱わされるものとして、次のような原理だよ

(B.du.

> $\tau \wedge \delta$. > $t \cdot \delta$. $\alpha \cdot \delta (t)$ $\alpha \cdot \delta (t) = \delta_{1} \alpha^{0} + \delta_{4} \alpha^{7} + \dots + \delta_{1} \alpha^{2} + \delta_{0} \alpha^{7}$ $= \delta_{4} \alpha^{7} + (\delta_{5} + \delta_{7}) \alpha^{6} + (\delta_{4} + \delta_{7}) \alpha^{5} + (\delta_{5} + \delta_{7}) \alpha^{4}$ $+ \delta_{2} \alpha^{5} + \delta_{1} \alpha^{2} + \delta_{0} \alpha$

たので、第10図に示したようなエクスクルシ ナオフルートEX-ORas~EX-ORas を用いて実現され、 B以が入力されれはα·B似 なる乗舞出力を得る ことができる。

なか、α² 乗算図路 δ ρ 、α³ 乗算回路 δ σ 化ついても上述したα 乗算回路 δ σ 化準じて容易に構成することができる。

而して、以上の構成において被除数 α^1 、除数。 α^1 は直接あるいは α , α^2 , α^3 の各乗算回路 s s \sim s o を介して α^4 乗算回路である 線形 シフトレ シスタ Δ_1 \sim Δ_4 、 B_1 \sim B_4 化 尚初

K セットされた後、クロックパルスCpが入力さ

れる毎に a⁴が乗じられる。そして、 C の過程でレジスタ A L ~ A a の 9 ちのいずれかの内容が a²⁸⁵ = 1 になった時点で 1 検出回路 5 4~ 8 7 によりクロックパルスCpが停止されると共に、上記 a²⁸⁵ = 1 になったレジスタ A L ~ A a に対 応するレジスタ B L ~ B a の内容が飲算結果としてアンド回路 6 1~ 6 4、オア回路 6 8 を介・して出力される。

次に、具体例として α^{10} $\div \alpha^{240}$ $\Rightarrow \alpha^{10-240}$ $\Rightarrow \alpha^{25}$ なる除算を実行する場合について説明する。 との場合レジスタ $A_1 \sim A_4$ 、 $B_1 \sim B_4$ は

$$\begin{pmatrix} A_1 : \alpha^{240} & & \\ A_2 : \alpha^{241} & & \\ A_3 : \alpha^{242} & & \\ A_4 : \alpha^{248} & & \\ A_4 : \alpha^{15} \end{pmatrix}$$

のように当初セットされるがクロックペルスCp が3個人ってきた状態で $\alpha^4 \cdot \alpha^4 \cdot \alpha^4 = \alpha^{12}$ が乗じ られることにより $\begin{pmatrix} A_{1 & 1} & \alpha^{252} & & & \\ A_{2 & 1} & \alpha^{255} & & & \\ A_{3} & 1 & \alpha^{254} & & & \\ A_{4} & 1! & \alpha^{265} & & & \\ A_{4} & 1! & \alpha^{265} & & \\ \end{pmatrix}$

の如く、レジスタA。がα²⁵⁵ = 1 となるのでこれに対応するレジスタB。の内容α²⁵ が簡として出力されるものである。

とのように、1回年にのを乗じることにより、必要となるのの集算回数を最高でも63回(の1-cm)に任欲した状態で所期の除算を乗算処理でなせるものである。

また、 線形シフトレジスタを 5 組、 α^5 乗算回路を使用すれば、必要となる α の乗算回数を最高でも 5 0 回に低級し得る如く、 それを拡張することによって 5 5 なる低級を図ることが可能である。

なお、この発明は上記し且つ図示した実施例のみに限定されることなく、...この発明の要旨を 途脱しない範囲で截々の変形や適用が可能であ ることは言う迄もない。

具体例を示す構成図、第7図乃至第10図はそれぞれ第6図のα⁴乗算回路を構成する線形シフトレジスを部および1検出回路部、アンド回路部、オア回路部、α⁴乗算回路の具体例を示す構成図である。

出願人代理人 弁理士 鈴 江 貮 彦

特問昭58-219647 (11)

例えば、テープ PCM 等のデジタル化された情報の伝送や記録再生ジステム、計算機ジステム等でガロア体による代数演算を必要とする機器に任政するものである。

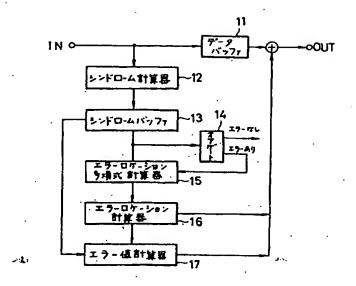
(発明の効果)

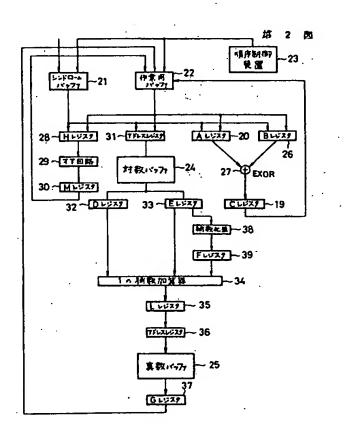
従って、以上評述したようにこの発明によれば、大容量のメモリを必要とする対数パッファを再いることなくガロア体にかける除算をなし得るようにし、以って構成の簡易化ならびに低価格かよび高速処理化に容与し得るようにした極めて良好なるガロア体にかける除其機量を提供することが可能となる。

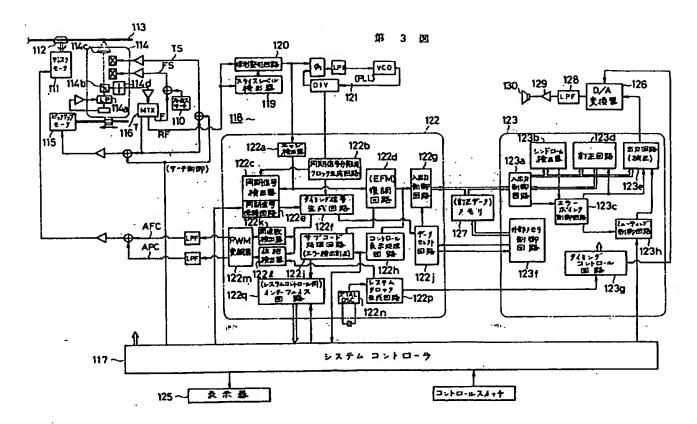
4. 図面の簡単な説明

第1図はリードソロモン符号の復号システムを示す板路構成図、第2図は従来のエラーロケーション多項式計算器を示す構成図、第3図はこの発明が適用されるDAD 再生装置の観要を示す構成図、第4図はこの発明の一実施例を示す構成図、第5図は第4図の乗算装置部の具体例を示す構成図、第6図は第4図の映算装置部の

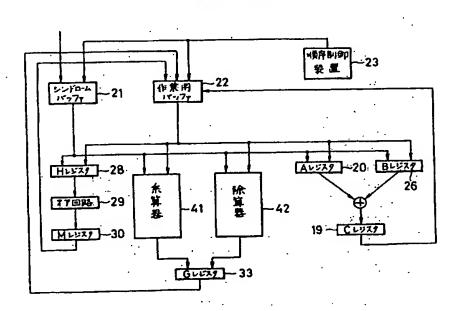
第 1 図



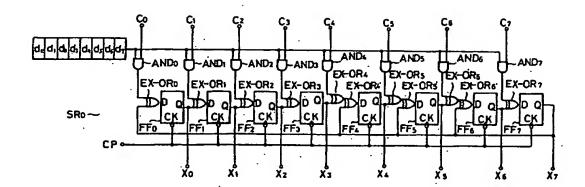


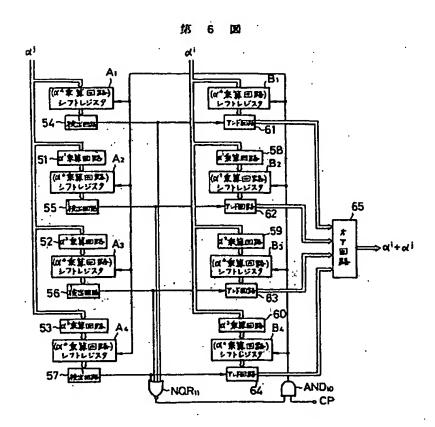


郑 4 図

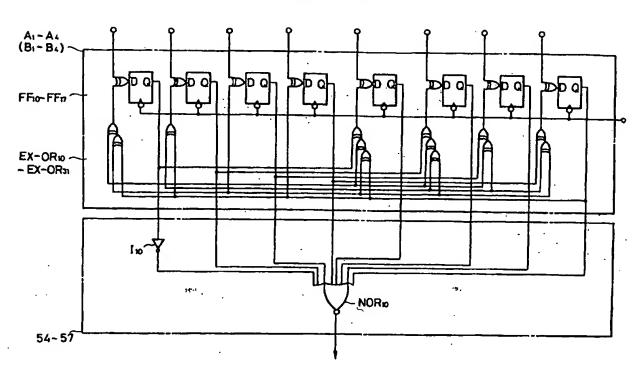


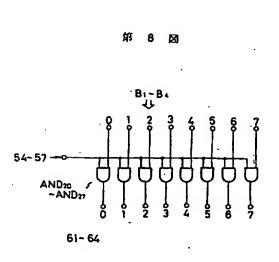
第 5 図

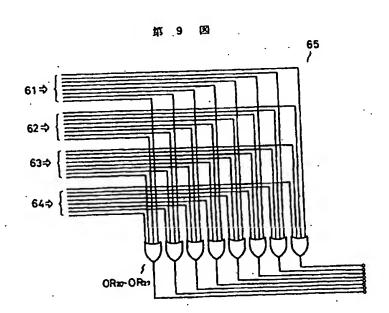












第 10 図

